

Just a little of that human touch

Daniel Genkin

Technion and Tel Aviv University

Itamar Pipman

Tel Aviv University

Eran Tromer

Tel Aviv University



TEL AVIV UNIVERSITY

Laboratory for Experimental Information Security

CRYPTO'13 rump session post-Snowden advisory

Using full-disk encryption
Email with PGP
Elliptic curves in your browser for forward secrecy

Hardware tokens for crypto
Using bitcoins to pay

Everybody use **CRYPTO**
Screw the NSA



Earlier: acoustic cryptanalysis

RSA 4096-bit key extraction using microphones



Sound propagation is limited in range and frequency.
What other channels are out there?

Power? Electromagnetic?

- PCs:
 - Multi-GHz clockrate
 - Many electrically noisy electronics
 - Limited physical access
- Full-bandwidth attacks are hard
- **Low-bandwidth attacks work!**
But unwieldy:
 - **Power analysis**
requires disconnecting the target from its power supply
 - **Electromagnetic analysis**
has short range, fiddly antenna placement



Ground-potential analysis

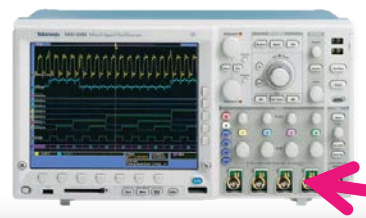
- **Attenuating EMI emanations**
“Unwanted currents or electromagnetic waves?
Dump them to the circuit ground!”
(Bypass capacitors, RF shields, ...)
- Device is grounded, but its “ground” potential fluctuates relative to the mains earth ground.



affects Computation
connected to device ground
connected to conductive chassis
shielded cables



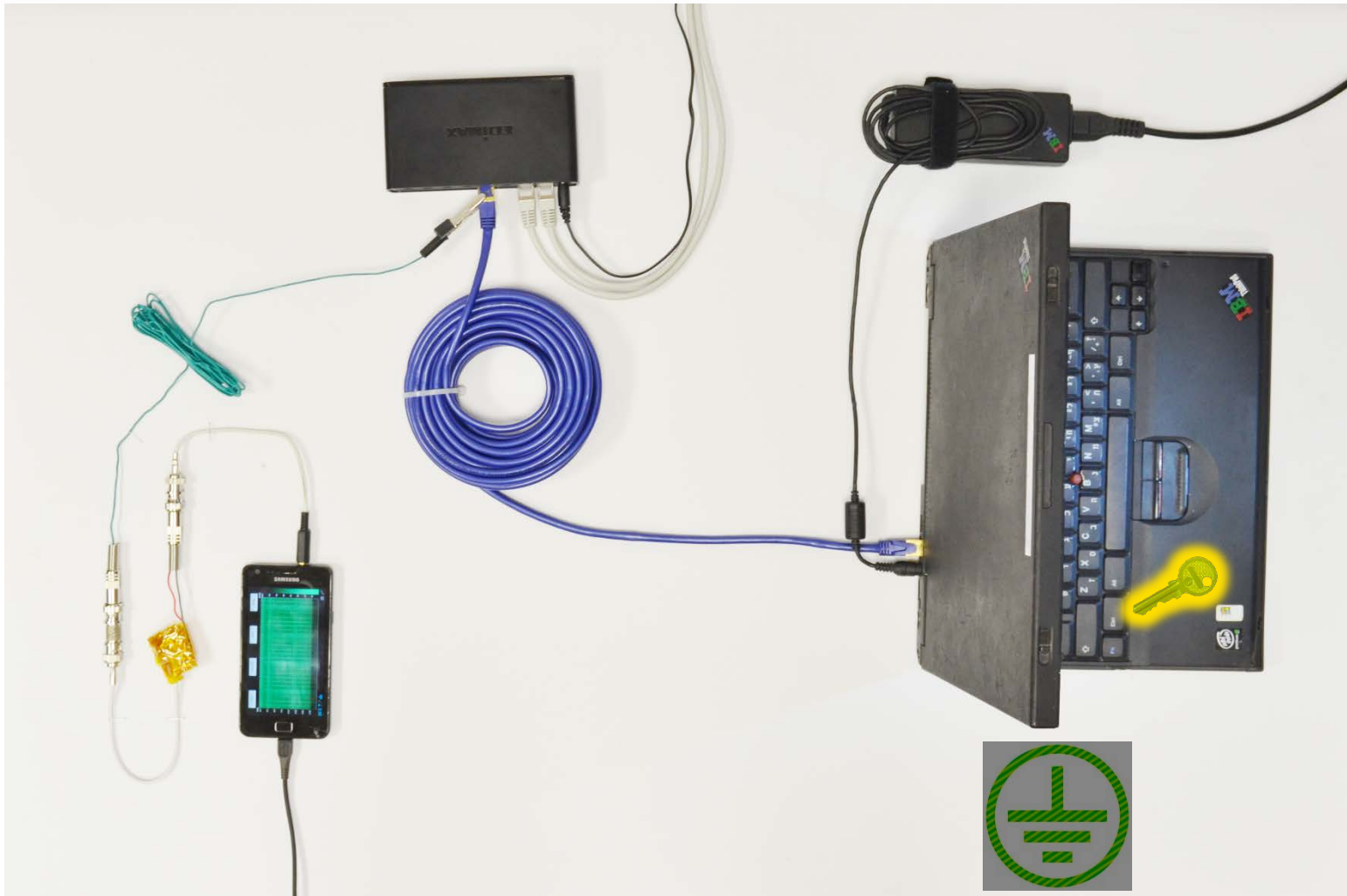
Even when no data, or port is turned off.



Live demo

- Meanwhile, on the other side of the VGA cable...
- Human touch key-extraction
- Luchtime attack
- Equipment

Key extraction on far side of Ethernet cable using a mobile phone



www.tau.ac.il/~tromer/handsoff

Rejected from ePrint. Accepted to CHES 2014.

CVE-2014-5270

RSA, ElGamal key extraction from GnuPG in a few seconds.



Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs (extended version)

Daniel Genkin
Technion and Tel Aviv University
danielg3@cs.technion.ac.il

Itamar Pipman
Tel Aviv University
itamarpi@tau.ac.il
July 31, 2014

Eran Tromer
Tel Aviv University
tromer@tau.ac.il

Abstract

We demonstrate physical side-channel attacks on a popular software implementation of RSA and ElGamal, running on laptop computers. Our attacks use novel side channels, based on the observation that the “ground” electric potential, in many computers, fluctuates in a computation-dependent way. An attacker can measure this signal by touching exposed metal on the computer’s chassis with a probe, wire, or even with a bare hand. The signal can also be measured at the remote end of Ethernet, VOIP, and USB cables. In this paper, based on signal processing, we have extracted 4096-bit RSA keys from these channels, as well as via power analysis and side-channel analysis. Various noise sources